

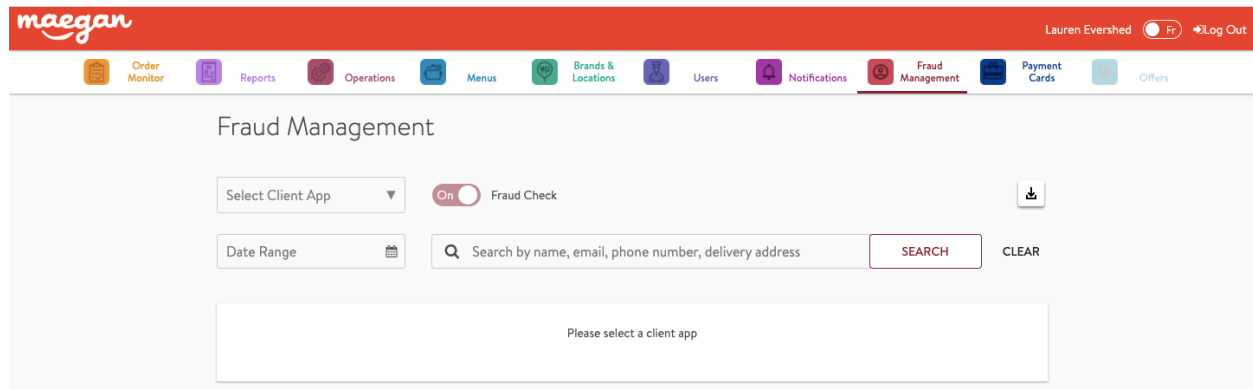
Fraud Management

Summary

Fraud Management is a feature in the Maegan back-office created to help manage fraudulent users and protect your company from fraudulent payments. This feature allows you to view payment activity from users accounts and blacklist or whitelist them based on the data presented.













How to Use













1. Go to the Fraud Management tab in back-office
2. Select Client App (only for users with Admin permissions for the client app)
3. Turn ON/OFF Guest Fraud Check
 1. If the toggle is ON, the system will automatically check and blacklist fraudulent customers
 2. If toggle is OFF, the system will NOT automatically check or blacklist fraudulent customers
4. Select the dates in which you like view customers who have placed orders
5. Search for a specific user if desired
6. Results will display based on search inputs






Payment Activity and Status

Payment Activity

Payment Activity	Definition	Preview				
No status	<ul style="list-style-type: none"> Regular customer - has not been whitelisted or blacklisted. Customer may be automatically marked as blacklisted if fraudulent activity is detected. <ul style="list-style-type: none"> <i>(highRiskFraudFlag=0)</i> 	N/A				
Blacklisted	<ul style="list-style-type: none"> User is high risk for fraud A customer is automatically blacklisted if they changed their credit card more than 3 times with cards registered to multiple postal codes and different names Credit Cards are identified by last 4 digits, as we never receive full card number Blacklisted customers may not add or update credit cards Blacklisted customer may not place orders on the respective client app <i>(highRiskFraudFlag=1)</i> 	<table border="1"> <thead> <tr> <th>Payment Activity</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td> Blacklisted</td> <td> Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM</td> </tr> </tbody> </table>	Payment Activity	Status	 Blacklisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM
Payment Activity	Status					
 Blacklisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM					
Blacklisted - phone number	<ul style="list-style-type: none"> Any account that uses this phone number will be blacklisted and considered a high risk for fraud Accounts with this phone number will not be able to place orders, add cards or reload cards 	<table border="1"> <thead> <tr> <th>Payment Activity</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td> Blacklisted</td> <td> Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM</td> </tr> </tbody> </table>	Payment Activity	Status	 Blacklisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM
Payment Activity	Status					
 Blacklisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM					

Blacklisted - address	<ul style="list-style-type: none"> • If a user is blacklisted by their delivery address they are unable to place a delivery order with this address • A user with this delivery address can still order for pickup 	<table border="1"> <thead> <tr> <th data-bbox="909 258 1229 369">Payment Activity</th> <th data-bbox="1229 258 1578 369">Status</th> </tr> </thead> <tbody> <tr> <td data-bbox="909 369 1229 577">  Blacklisted </td> <td data-bbox="1229 369 1578 577">  Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM </td> </tr> </tbody> </table>	Payment Activity	Status	 Blacklisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM
Payment Activity	Status					
 Blacklisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:48 PM					
Whitelisted	<ul style="list-style-type: none"> • The system will not check this user account for fraudulent activities and the customer may continue to place orders • If user is whitelisted they still need to pass 3D Secure, but we allow all crypt types for them 	<table border="1"> <tbody> <tr> <td data-bbox="909 695 1229 903">  Whitelisted </td> <td data-bbox="1229 695 1578 903">  Reviewed Admin Back-office, 26 Apr 2021, 03:49 PM </td> </tr> </tbody> </table>	 Whitelisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:49 PM		
 Whitelisted	 Reviewed Admin Back-office, 26 Apr 2021, 03:49 PM					

Status

Status	Definition	Preview		
Reviewed	<ul style="list-style-type: none"> • An operator has reviewed the customer's account details and has either blacklist/whitelisted them • If a customer was reviewed, it will display the user who reviewed their account and date/time of review 	<table border="1"> <thead> <tr> <th data-bbox="1172 1289 1578 1381">Status</th> </tr> </thead> <tbody> <tr> <td data-bbox="1172 1381 1578 1564">  Reviewed Admin Back-office, 18 May 2021, 05:25 PM </td> </tr> </tbody> </table>	Status	 Reviewed Admin Back-office, 18 May 2021, 05:25 PM
Status				
 Reviewed Admin Back-office, 18 May 2021, 05:25 PM				

Customer Details

If you choose to edit a customer's profile you can Blacklist customer, Whitelist customer or Blacklist the phone number or delivery address only.

Order Monitor
 Reports
 Operations
 Menus
 Brands & Locations
 Users
 Notifications
 Guest Payments

Cancel Save

Customer Details

Guest Info

First Name	Jane	Last Name	Doe
Email	jane.doe@gmail.com	Phone	4161234567
Notifications	Receives emails and push notifications and texts		Credit Cards

Actions

Blacklist Customer
 Whitelist Customer

Blacklist :

Phone Number
4161234567

Actions

Blacklist Customer
 Whitelist Customer

Blacklist :

Phone Number
647.879.6353

Delivery Address
 36 King Street, Charleston, 29401

Guest Info

Item	Definition
First Name	<i>First name registered to user account</i>
Last Name	<i>Last name registered to user account</i>
Email	<i>Email registered to user account</i>
Phone	<i>Phone number registered to user account</i>
Notifications	<i>If on app, if they opted in to receiving push notifications</i>
Credit Cards	<i>Credit card processor and last 4 digits of credit card on file (ex. Visa ****1234)</i>

Credit Card Add and Removal Activity

Operation Name	
Value	Definition
Add Vault Record	<i>Customer added a new credit card to profile</i>
Update Vault Record	<i>Customer updated credit card on their profile</i>
Three D Secure Check Required	<i>Customer is required to go through 3D secure</i>
Three D Secure Check	<p><i>Customer went through 3D secure check</i></p> <p><i>If Three D secure check does not appear after Three D secure check required, the user chose not to go through 3D secure check. This may be an indicator of a fraudulent user.</i></p> <p><i>ECI indicator (see below)</i></p>
Payment Card Balance Transfer	<i>Customer loaded funds onto gift card from a credit card</i>

Device ID

- ID of device where operation has taken place

Time Stamp

- Date and Time of operation

Cardholder Name

- Name on Card

Invocation Source

- Where in app payment card registration took place
- Web Ordering, Account Profile, Mobile ordering

Card Type

- Credit card processor: Visa, MasterCard, American Express , Discover, JCB

Street

- Street address associated with card entered by the user

Postal/ Zip Code

- Postal/Zip code associated with Credit card billing address (NOT the delivery address)

CVD Response - Card Validation Digits response

Card Security Codes are the 3-digit numbers located on the back of Visa ([CVV2](#)), MasterCard ([CVC 2](#)) and Discover (CID) cards, in or around the signature panel, and the 4-digit numbers located on the front of American Express (CID) cards, above the card account number. Card Security Codes help verify that the customer is in a physical possession of a valid card during a card-not-present transaction. Similarly to the AVS, the merchant includes the security code with the authorization request and the issuer replies with a response code, as listed in the table below:

The responses that are received from CVD verifications are intended to provide added security and fraud prevention, but the response itself will not affect the issuer’s approval of a transaction. Upon receiving a response, the choice to proceed with a transaction is left entirely to the merchant. Please note that all responses coming back from these verification methods are not direct indicators of whether a merchant should complete any particular transaction. The responses should not be used as a strict guideline of which transaction will approve or decline.

CVD verification is only applicable towards Visa, MasterCard, Discover, American Express, JCB, and UnionPay card transactions.

<https://developer.moneris.com/More/Testing/CVD%20Result%20Codes>

CVD Result Definitions	
M	Match

N	No Match
P	Not Processed
S	CVD should be on the card, but Merchant has indicated that CVD is not present.
U	Issuer is not a CVD participant
Y	Match for AmEx/JCB only
D	Invalid security code for AmEx/JCB
Other	Invalid response code

AVS Response - Address Verification Service response

AVS enables merchants who accept credit card payments in a non-face-to-face setting to compare the billing address (the address to which the card issuer sends its monthly statement for that account) provided by a customer to the billing address on the card issuer's file before processing a transaction. After comparing the provided address with the one they have on file for their cardholder, the card issuer responds by issuing one of the AVS Response code listed in the table below.

AVS verification is only applicable towards Visa, MasterCard, Discover, and American Express card transactions. This verification method is not applicable towards any other card type.

<https://developer.moneris.com/More/Testing/AVS%20Result%20Codes>

AVS Result Definitions				
A	Street address matches but postal code does not, or the request does not include the postal code.	Address matches, postal code does not.	Address matches, five-digit postal code matches	Billing address matches, zip code does not.
B	Street address matches. Postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)	N/A	N/A	N/A
C	Street address and postal code not verified due to incompatible formats. (Acquirer sent both street address and postal code.)	N/A	N/A	N/A

D	Street addresses and postal codes match.	N/A	N/A	Customer name incorrect, postal code matches
E	N/A	N/A	N/A	Customer name incorrect, billing address and postal code match
F	N/A	N/A	N/A	Customer name incorrect, billing address matches.
G	Address information not verified for international transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, or Visa performs AVS on behalf of the issuer and there was no address record on file for this account.	N/A	Address information not verified for international transaction	N/A
I	Address information not verified.	N/A	N/A	N/A
K	N/A	N/A	N/A	Customer name matches
L	N/A	N/A	N/A	Customer name and postal code match.
M	Street address and postal code match.	N/A	N/A	Customer name, billing address, and postal code match.

N	No match. Acquirer sent postal/ZIP code only, or street address only, or both postal code and street address. Also used when acquirer requests AVS but sends no AVS data.	Neither address nor postal code match.	Neither address nor postal code match.	Billing address and postal code do not match.
O	N/A	N/A	N/A	Customer name and billing address match
P	Postal code match. Acquirer sent both postal code and street address but street address not verified due to incompatible formats.	N/A	N/A	N/A
R	Retry: system unavailable or timed out. Issuer ordinarily performs AVS but was unavailable. Available for U.S. issuers only.	Retry; system unable to process.	N/A	System unavailable; retry.
S	Not applicable. If present, replaced with G (for international) or U (for domestic) by V.I.P. Available for U.S. Issuers only.	AVS currently not supported.	AVS currently not supported.	AVS currently not supported.
T	N/A	N/A	Nine-digit zip code matches, address does not match.	N/A
U	Address not verified for domestic transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, or Visa performs AVS on behalf of the issuer and there was no address record on file for this account.	No data from Issuer/Authorization system.	Retry; system unable to process.	Information is unavailable.

W	Not applicable. If present, replaced with 'Z' by Visa. Available for U.S. issuers only.	For U.S. Addresses, nine-digit postal code matches, address does not; for address outside the U.S. postal code matches, address does not.	No data from Issuer/Authorization system	Customer name, billing address, and postal code are all correct.
X	Not applicable. If present, replaced with Y by V.I.P. Available for U.S. issuers only.	For U.S. addresses, nine-digit postal code and addresses matches; for addresses outside the U.S., postal code and address match.	Address matches, nine-digit postal code matches	N/A
Y	Street address and postal code match.	For U.S. addresses, five-digit postal code and address matches.	Address matches, postal code does not	Billing address and postal code both match
Z	Postal/Zip matches; street address does not match or street address not included in request.	For U.S. addresses, five-digit postal code matches, address does not match.	Five-digit postal code matches, address does not	Postal code matches, billing address does not.

Message

- Response message related to operation from bank

Three D Secure Object

Please note, Three-D secure is currently only available for clients using Moneris as their payment provider.

5	<ul style="list-style-type: none"> • Fully authenticated • There is a liability shift, and the merchant is protected from chargebacks 	<ul style="list-style-type: none"> • Fully authenticated • There is a liability shift, and the merchant is protected from chargebacks. 	<ul style="list-style-type: none"> • Fully authenticated • There is a liability shift, and the merchant is protected from chargebacks.

6	<ul style="list-style-type: none"> • Visa Secure has been attempted • There is a liability shift, and the merchant is protected from certain chargebacks on fraudulent transactions 	<ul style="list-style-type: none"> • MasterCard Identity Check has been attempted • There is a liability shift, and the merchant is protected from certain chargebacks on fraudulent transactions 	<ul style="list-style-type: none"> • American Express SafeKey has been attempted • There is a liability shift, and the merchant is protected from certain chargebacks on fraudulent transactions
7	<ul style="list-style-type: none"> • Non-Visa Secure transaction • No liability shift • Merchant is not protected from chargebacks 	<ul style="list-style-type: none"> • Non-MasterCard Identity Check transaction • No liability shift • Merchant is not protected from chargebacks 	<ul style="list-style-type: none"> • Non-American Express SafeKey transaction • No liability shift • Merchant is not protected from chargebacks

Restaurant Name

- Name of the location

Payment Card Program Name

- For additional payment programs outside of credit payments only (ex. Gift cards, student payments)

Successful

- If True, operation was successful